UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/978,113	10/15/2001	Eng-Whatt Toh	20735-05502	3747

7590 03/31/2005

ROBERT N . BLACKMAN
MEREK , BLACKMORE & VOORHEES , LLC
673 S . WASHINGTON ST .
ALEXANDRIA, VA 22314

EXAMINER	
JACK, TODD M	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 03/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/978,113	TOH ET AL.	
	Examiner	Art Unit	
	Todd M Jack	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/15/2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *10 June 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/02, 5/02, 6/02, 10/02,*
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☒ Other: *Office Action*.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 3, 12-14, 16, 24, and 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Owens et al. (6,338,140 B1)

Claim 1: Owens (6,338,140 B1) teach a device identification is transmitted from the communications device to the authentication engine prior to transmitting the dynamic personal identification number, which is produced by cryptographic keys input and a cryptographic algorithm (col. 9, lines 5-18), a stored secret key (i.e. private key) and an appropriate cryptographic key for the calling subscriber (i.e. public key) (col. 15, lines 28-37) where the valid cryptographic key mapped to the possible device identification number is included in the database (col. 9, lines 55-66); Thus, the cryptographic key has characteristics of a public key such as being possibly available to all users, etc., transmitting the dynamic personal identification number to the authentication engine via a mobile switching center in the communications network (col. 9, lines 22-26), crypto keys (which may be public keys) being associated with various mobile stations (i.e. access systems) where the entire private-public key pair may be associated with a mobile station (i.e. access system), crypto keys directed toward the

crypto algorithm in the network to perform authentication (col. 2, lines 27-39) where the access system may use crypto keys of the private-public key pair, two access gateways are required to connect to either or both such access gateways (col. 19, lines 17-21) for transmission of data, the authentication engine may include a communications server and an authentication server communicating where the communications server determining a cryptographic key corresponding to the received device identification number (col. 9, lines 27-34), transmitting the dynamic personal identification number to the authentication engine via a mobile switching center in the communications network (col. 9, lines 22-26), the communications and authentication server may receive the device identification, perform the step of determining a cryptographic key corresponding to determining a cryptographic key corresponding to the received device identification number and perform the personal identification number comparing step (col. 9, lines 44-50), the validation system includes one or more communication servers linked to an authentication server and a processor (col. 9, lines 55-67 and col. 10, lines 1-2) where the processor may be a switch system, and the system includes an interoperability unit communicating with the communications server and the authentication server (col. 10, lines 13-16).

Claim 3: Further, Owens teach an authentication scheme occurring in a mobile switching center connected to various nodes equipped with a cryptographic algorithm (col. 3, lines 4-9).

Claim 12: Further, Owens teach that two gateways are required, one for each TCP/IP network to IS-41 network interface where the authentication engine according to the instant invention may be connected to either or both such access gateways, converting the message into an IS-41 message and sends it to a mobile switching center (col. 19, lines 16-36).

Claim 13: Further, Owens teach access gateways, converting the message into an IS-41 message and sends it to a mobile switching center which routes the message to the base station, which transmits the message to the mobile station (col. 19, lines 16-36). The base station acts as an application proxy.

Claim 14: Further, Owens teach a cryptographic algorithm utilizing numerical inputs and produce numerical outputs (col. 19, lines 61-64). The algorithm acts as an application proxy processing data based upon a define series of steps.

Claim 16: Owens teach transmitting the dynamic personal identification number to the authentication engine via a mobile switching center in the communications network (col. 9, lines 22-26), two gateways are required, one for each TCP/IP network to IS-41 network interface where the authentication engine according to the instant invention may be connected to either or both such access gateways, converting the message into an IS-41 message and sends it to a mobile switching center (col. 19, lines 16-36) where the gateways act as nodes, password generators cryptographically process two or more inputs which include a cryptographic key to generate an output comprising a personal

identification number (col. 10, lines 38-43), crypto keys directed toward the crypto algorithm in the network to perform authentication (col. 2, lines 27-39) where the access system may use crypto keys of the private-public key pair, and a system includes an interoperability and translating communications signal between the communications network of the subscriber and one communications network where the interoperability unit communicates with the communication server and the authentication server (col. 10, lines 13-31).

Claim 24: Further, Owens teach access gateways, converting the message into an IS-41 message and sends it to a mobile switching center which routes the message to the base station, which transmits the message to the mobile station (col. 19, lines 16-36). The base station acts as an application proxy.

Claim 25: Further, Owens teach a wireless backbone network connecting a plurality of nodes (Fig. 5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 4, 17, 27, 28, 37-42, 50, and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Blumenau (6,493,825 B1).

Claim 2: Owens teach a stored secret key (i.e. private key) and an appropriate cryptographic key for the calling subscriber (i.e. public key) (col. 15, lines 28-37) where the valid cryptographic key mapped to the possible device identification number is included in the database (col. 9, lines 55-66); Thus, the cryptographic key has characteristics of a public key such as being possibly available to all users, etc. Owens teach a switch system which issues to an access system the access system's private-public key pair and transmitting the dynamic personal identification number to the authentication engine via a mobile switching center in the communications network (col. 9, lines 22-26), two gateways are required, one for each TCP/IP network to IS-41 network interface where the authentication engine according to the instant invention may be connected to either or both such access gateways, converting the message into an IS-41 message and sends it to a mobile switching center (col. 19, lines 16-36) where the gateways act as nodes. Owens fails to teach a switch system issues the private-public key pair. Blumenau teach the use of any sequence of encryption operations such as the public/private key system (col. 37, lines 62-67) used by the port adapter and the host controller (col. 38, lines 1-5). The switch system issues to various access systems the public-private key pair for that particular system.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including a private-public key pair. This modification would have been obvious to a person having

ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Blumenau, in order to provide the means to encrypt/decrypt the messages to and from the nodes.

Claim 4: Further, Owens teach a node is identified as the nodes of the fabric port are connected through the fabric (col. 19, lines 16-21).

Claim 17: Further, Owens fails to teach a key module is further adapted to perform the step of issuing a private-public key pair to an access system. Blumenau teach the use of any sequence of encryption operations such as the public/private key system (col. 37, lines 62-67) used by the port adapter and the host controller (col. 38, lines 1-5).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including a private-public key pair. This modification would have been obvious to a person having ordinary skill in the art. They would have been motivated to do so, as suggested by Blumenau, in order to provide the means to encrypt/decrypt the messages to and from the nodes.

Claim 27: Owens teach a node of a fabric port interconnected to other nodes through a fabric where the node is interrogated about the identity of other nodes (col. 9, lines 19-34) where interrogation may be accomplished in a cryptographic manner, the authentication engine may include a communications server and an authentication

server communicating where the communications server determining a cryptographic key corresponding to the received device identification number (col. 9, lines 27-34), a node of a fabric port can be interrogated about the identity of other nodes of the fabric to which the nodes of the fabric port is directly connected to through the fabric (col. 9, lines 19-26) where the interrogation leads to a secure network. Owens fails to teach a key module for accessing a private-public key pair of a user of the access system. Blumenau teaches the use of any sequence of encryption operations such as the public/private key system (col. 37, lines 62-67) used by the port adapter and the host controller (col. 38, lines 1-5). The switch system issues to various access systems the public-private key pair for that particular system.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including a private-public key pair. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Blumenau, in order to provide the means to encrypt/decrypt the messages to and from the nodes.

Claim 28: Further, Owens fails to teach a key module is adapted to perform the generating of a private-public key pair of a user. Blumenau teach the use of any sequence of encryption operations such as the public/private key system (col. 37, lines 62-67) used by the port adapter and the host controller (col. 38, lines 1-5).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including a private-public key pair. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Blumenau, in order to provide the means to encrypt/decrypt the messages to and from the nodes.

Claim 37: Further, Owens teach two access gateways are required to connect to either or both such access gateways for transmission of data (col. 19, lines 16-21).

Claim 38: Further, Owens teach an access gateway sends a converted message to the mobile switching center which routes the message to the base station, which transmits the message to a mobile station (col. 19, lines 22-36).

Claim 39: Owens teach a RPA engine is the central processor that is used to authenticate wireless subscribers in the environment primarily when the local serving mobile switching center is not authentication capable where the RPA (random pin authentication engine) performs various functions while connected to the network (col. 13, lines 15-23). The functions may be accomplished through the processor by program code. Owens teaches a TCP/IP-based network may interconnect two remotely based wireless networks as to transport short messages between two wireless networks (col. 19, lines 8-14), crypto keys directed toward the crypto algorithm in the network to

perform authentication (col. 2, lines 27-39) where the access system may use crypto keys of the private-public key pair, determining a cryptographic key to be used to transmit a personal identification number to the authentication engine via a mobile switching center in the communications network (col. 9, lines 19-26), authentication may be performed when accessing mobile switching centers (col. 7, lines 38-40), the invention supports the interworking of authenticating an non-authenticating network or network element and supports a constant blanket of cryptographic coverage (col. 7, lines 42-45), wireless communication network requiring user authentication for authorizing and validate user identities (col. 18, lines 42-45) where a public key may be used to accomplish these tasks (col. 2, lines 27-39), wireless communications networks requiring user authentication for authenticating for access using an authentication engine according to the instant invention requiring to be operatively connected in a standard configuration to an access point or authorization point to validate user identities (col. 18, lines 38-49), and the communications network may include one or more computer networks requiring user authentication for access to the Internet and local/wide networks that may be connected to the Internet (col. 18, lines 50-67). Owens fails to teach associating each of a plurality of access systems with a public key from a private-public key pair associated with the access system. Blumenau teaches the use of any sequence of encryption operations such as the public/private key system (col. 37, lines 62-67) used by the port adapter and the host controller (col. 38, lines 1-5). The switch system issues to various access systems the public-private key pair for that particular system.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including a private-public key pair. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Blumenau, in order to provide the means to encrypt/decrypt the messages to and from the nodes.

Claim 40: Further, Owens teach a computer medium connected to a cellular network with the use of crypto-keys in a challenge-response authentication scheme (Fig. 2).

Claim 41: Further, Owens teach a wireless network connecting with a various amount of nodes by a challenge-response authentication scheme (Fig. 5).

Claim 42: Further, Owens teach two access gateways, one for each network to a network interface which are connected by either or both such access gateways (col. 19, lines 16-21).

2

Claim 50: Further, Owens teach anyone with World Wide Web access may enter a mobile subscriber's telephone number and a text message at a site. The message is sent over the TCP network to the appropriate IS-41 network. The gateway converts the message into an IS-41 message and sends it to the mobile switching center. (col. 19, lines 22-31).

Claim 51: Further, Owens teach a message being sent over the TCP network to the appropriate IS-41 network. The access gateway converts the message into an IS-41 message and sends it to the mobile switching center, which routes the message to the base station. (col. 19, lines 27-30) The TCP network provides an access to the switching center via access gateway, which acts as an application proxy.

Claims 5, 8, 18, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Dancs et al. (6,112,305)

Claim 5: Further, Owens fails to teach comprising the switch system performing the step of: using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system. Dancs teach the network connector validates the contents of the smart card by using the public key found in the ISP certificate (col. 6, lines 65-67) and the contents are certified with a private key that only the manufacturer or trusted root authority holds (col. 6, lines 54-56).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including a private-public key to authenticate the system. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Dancs, in order to provide the means to authenticate.

Claim 8: Further, Owens fails to teach the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key. Dancs teaches that if there is a Personal Identification Number (PIN) of the user, which is compared to the PIN of the smart card. When a match does not occur, then the process stops. (col. 7, lines 20-25) The PIN is used as an encryption key.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including an encryption key check. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Dancs, in order to reject improper encryption keys set forth to overcome the security protections.

Claim 18: Further, Owens fails to teach the authentication module is further adapted to perform the step of: using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system. Dancs teach the network connector validates the contents of the smart card by using the public key found in the ISP certificate (col. 6, lines 65-67).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including a

private-public key to authenticate the system. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Dancs, in order to provide the means to authenticate.

Claim 21: Further, Owens fails to teach the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key. Dancs teaches that if there is a Personal Identification Number (PIN) of the user, which is compared to the PIN of the smart card. When a match does not occur, then the process stops. (col. 7, lines 20-25) The PIN is used as an encryption key.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including an encryption key check. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Dancs, in order to reject improper encryption keys set forth to overcome the security protections.

Claims 43, 46, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Blumenau, and further in view of Dancs.

Claim 43: Further, Owens fails to teach program code adapted to perform the step of: using a switch system private key, in conjunction with an access system using a

corresponding switch system public key, to authenticate the switch system to the access system. Dancs teach the network connector validates the contents of the smart card by using the public key found in the ISP certificate (col. 6, lines 65-67), an enterprise signature is created by performing a secure hash on the enterprise contents and encrypting it with the enterprise private key (col. 20, lines 34-36).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including a private-public key to authenticate the system and a private key. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Dancs, in order to provide the means to authenticate.

Claim 46: Further, Owens fails to teach the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key. Dancs teach that if there is a Personal Identification Number (PIN) of the user, which is compared to the PIN of the smart card. When a match does not occur, then the process stops. (col. 7, lines 20-25) The PIN is used as an encryption key.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including an encryption key check. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated

to do so, as suggested by Dancs, in order to reject improper encryption keys set forth to overcome the security protections.

Claim 48: Further, Owens teach comprising program code adapted to perform the step of: storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature. Dancs teach verification of the contents of the smart card using the cryptographic signatures where the information to be stored in the RAM includes a digital signature portion (col. 8, lines 28-39).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including digital signatures with the data. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Dancs, in order to verify the origin of the data.

Claims 6, 15, 19, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Stevens (1994).

Claim 6: Further, Owens fails to teach the first and second cryptographically secure connections are each implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnection reference model. Stevens teach protocols are normally developed in layers, with each layer responsible for a different facet of the communications (pg. 1-7, "Layering").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including processes at different layers. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to process data in a modular fashion, thus allowing for quick and easy program alterations to occur.

Claim 15: Further, Owens fails to teach the policies for the application proxy are set by the access system. Stevens teach routing table entries point all datagrams to either the subnet or specific hosts on that subnet to the router. The router then knows how to get the datagrams to their final destination. (pg. 62, section 4.6)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by allowing the access system to set policies. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to allow various access systems to interface with a given proxy.

Claim 19: Further, Owens fails to teach the first and second cryptographically secure connections are each implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnection reference model. Stevens teach protocols

are normally developed in layers, with each layer responsible for a different facet of the communications (pg. 1-7, "Layering").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including processes at different layers. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to process data in a modular fashion, thus allowing for quick and easy program alterations to occur.

Claim 26: Further, Owens fails to teach the policies for the application proxy are set by the access system. Stevens teach routing table entries point all datagrams to either the subnet or specific hosts on that subnet to the router. The router then knows how to get the datagrams to their final destination. (pg. 60-62, section 4.6 &)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by allowing the access system to set policies. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to allow various access systems to interface with a given proxy.

Claims 7 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Stevens, further in view of Rowney (5,987,140).

Claim 7: Further, Owens fails to teach a first and second cryptographically secure network connections are each formed using at least one encryption key from a group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key. Rowney teach the computer system uses a random encryption key which is a symmetric encryption key (col. 13, lines 4-9) and asymmetric key pair such as a public key/private-key key pair where the message encrypted with one key of the key pair may only be decrypted with the other key of the same key pair (col. 13, lines 8-12).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by using an encryption key to secure a network connection. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Rowney, in order to provide for a network connection, which prevents an unauthorized entry.

Claim 20: Further, Owens fails to teach the cryptographically secure network connections are formed using at least one encryption key from the group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key. Rowney teach the computer system uses a random encryption key which is a symmetric encryption key (col. 13, lines 4-9) and asymmetric key pair such as a public key/private-key key pair where the message encrypted with one key of the

key pair may only be decrypted with the other key of the same key pair (col. 13, lines 8-12).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by securing the network. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Rowney, in order to provide for a network connection, which prevents an unauthorized entry.

Claim 9, 10, 11, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Rowney.

Claim 9: Further, Owens fails to teach a digest of at least a portion of the data and a digital signature of the first access system. Rowney teach combined contents of the combined block (col. 18, lines 53-59) and a digital signature for the combined contents of the combined blocks (col. 16, lines 53-67).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to include a digest and a digital signature. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Rowney, in order to possess all the components of a message and signature to authenticate it.

Claim 10: Further, Owens fails to teach compromising the switch system performing the step of time-stamping at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature. Rowney teach calculates a digital signature for the combined contents of the combined block comprising basic capture response and the signature public key certificate and appends the signature to the combination of the combined basic authorization request and the signature public key certificate (col. 18, lines 55-65). The digital signature may very well contain a time-stamp.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to include time-stamping a group. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Rowney, in order to form a digest containing all the pertinent information related to a message.

Claim 11: Further, Owens fails to teach compromising the switch system performing the step of time-stamping at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of the first access system. Rowney teach a merchant computer system calculates a digital signature for the combined contents of the combined block comprising basic capture response and the signature public key certificate and appends the signature to the combination of the combined basic

authorization request and the signature public key certificate (col. 18, lines 55-65). The digital signature may very well contain a time-stamp.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to include time-stamping a group. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Rowney, in order to form a digest containing all the pertinent information related to a message sent by the first access system.

Claim 22: Further, Owens fails to teach compromising the switch system performing the step of time-stamping at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature. Rowney teach calculates a digital signature for the combined contents of the combined block comprising basic capture response and the signature public key certificate and appends the signature to the combination of the combined basic authorization request and the signature public key certificate (col. 18, lines 55-65). The digital signature may very well contain a time-stamp.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to include time-stamping a group. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as

suggested by Rowney, in order to form a digest containing all the pertinent information related to a message.

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Stevens, further in view of Dancs.

Claim 23: Further, Owens fails to teach a tracking module for time stamping and storing at least one of the groups comprising the data, a digest of at least a portion of the data, and a digital signature of an access system. Stevens teach a timestamp option with the capability to record both IP addresses and time-stamps (pg. 95-96, section 95-96, section 7.4).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to include time-stamping a group. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to form a digest containing all the pertinent information related to a message.

Dancs teaches the use of a cryptographic signature appended to the contents of the smart card (col. 8, lines 28-39).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to use a signature for an identifier. This modification would have been obvious to a person

having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to be able to identify an access system.

Claims 30, 34, 35, 36, 44, 52, and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view Blumenau, further in view of Stevens.

Claim 30: Further, Owens fails to teach the cryptographically secure network connection is implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and session layer of the Open Systems Interconnect reference model. Stevens teach protocols are normally developed in layers, with each layer responsible for a different facet of the communications (pg. 1-7, "Layering").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including processes at different layers. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to process data in a modular fashion, thus allowing for quick and easy program alterations to occur.

Claim 34: Further, Owens fails to teach the policies for the application proxy are set by the access system. Stevens teach routing table entries point all datagrams to either the subnet or specific hosts on that subnet to the router. The router then knows how to get the datagrams to their final destination. (pg. 60-62, section 4.6)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by allowing the access system to set policies. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to allow various access systems to interface with a given proxy.

Claim 35: Further, Owens fails to teach the secure-network-connection application proxy is accessed by more than one client system. Stevens teach routing table entries point all datagrams to either the subnet or specific hosts on that subnet to the router. The router then knows how to get the datagrams to their final destination. (pg. 62, section 4.6)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by allowing specific hosts to access the proxy. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to allow various systems to access the proxy, thus making the messages available to more than one individual via the proxy.

Claim 36: Further, Owens fails to teach the secure-network-connection application proxy processes data initiated from a client system and data intended for the client

system based upon predefined policies. Stevens teaches routing directs datagrams to other hosts through the use of routing table entries (pg. 60-62, section 4.6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including a application proxy for processing based upon predefined policies. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to deal with all data on an individual basis.

Claim 44: Further, Owens fails to teach the cryptographically secure network connection is implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and session layer of the Open Systems Interconnect reference model. Stevens teach protocols are normally developed in layers, with each layer responsible for a different facet of the communications (pg. 1-7, "Layering").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including processes at different layers. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to process data in a modular fashion, thus allowing for quick and easy program alterations to occur.

Claim 52: Further, Owens fails to teach the secure-network-connection application proxy processes data initiated from a client system and data intended for the client system based upon predefined policies. Stevens teaches routing directs datagrams to other hosts through the use of routing table entries (pg. 60-62, section 4.6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including a application proxy for processing based upon predefined policies. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to deal with all data on an individual basis.

Claim 53: Further, Owens fails to teach the policies for the application proxy are set by the access system. Stevens teach routing table entries point all datagrams to either the subnet or specific hosts on that subnet to the router. The router then knows how to get the datagrams to their final destination. (pg. 62, section 4.6)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by allowing the access system to set policies. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to allow various access systems to interface with a given proxy.

Claims 29 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Blumenau, further in view Rowney (5,987,140).

Claim 29: Further, Owens fails to teach the authentication module is further adapted to perform the step of: using a switch system public key, in conjunction with the switch system using a corresponding switch system private key, to authenticate the switch system to the access system. Rowney teaches the encrypted state of encrypted random key is graphically shown by payment gateway public key lock. The gateway computer system concatenates encrypted combined block, encrypted random key, encrypted capture token an encrypted random key to form merchant authorization response (col. 15, lines 22-29).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by authenticating the switch system using keys. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Rowney, in order to allow the access system to verify that it is in contact with the appropriate switch system.

Claim 47: Further, Owens fails to teach a digest of at least a portion of the data and a digital signature of the first access system. Rowney teach combined contents of the combined block (col. 18, lines 53-59) and a digital signature for the combined contents of the combined blocks (col. 16, lines 53-67).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to include a digest and a digital signature. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Rowney, in order to possess all the components of a message and signature to authenticate it.

Claims 31 rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Blumenau, further in view of Stevens and Rowney.

Claim 31: Further, Owens fails to teach a first and second cryptographically secure network connections are each formed using at least one encryption key from a group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key. Rowney teach the computer system uses a random encryption key which is a symmetric encryption key (col. 13, lines 4-9) and asymmetric key pair such as a public key/private-key key pair where the message encrypted with one key of the key pair may only be decrypted with the other key of the same key pair (col. 13, lines 8-12).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by using an encryption key to secure a network connection. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have

been motivated to do so, as suggested by Rowney, in order to provide for a network connection, which prevents an unauthorized entry.

Claims 32 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Blumenau, further in view of Dancs.

Claim 32: Further, Owens fails to teach the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key. Dancs teach that if there is a Personal Identification Number (PIN) of the user, which is compared to the PIN of the smart card. When a match does not occur, then the process stops. (col. 7, lines 20-25) The PIN is used as an encryption key.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including an encryption key check. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Dancs, in order to reject improper encryption keys set forth to overcome the security protections.

Claim 33: Further, Owens fails to teach the secure network connection module is further adapted for generating at least one of the group comprising a digest of at least a portion of the data and a digital signature of the access system. Dancs teach a gateway computer system calculates a message digest over the contents of the request, the

encryption key certificate, and the signature public key certificate where the system decrypts the digital signature (col. 14, lines 5-13). The digest is the contents of the request.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by generating a digest and a digital signature. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Dancs, in order to verify the identity of authorized users of the system.

Claims 45 rejected under 35 U.S.C. 103(a) as being unpatentable over Owens in view of Blumenau, further in view of Stevens and Rowney.

Claim 45: Further, Owens fails to teach a first and second cryptographically secure network connections are each formed using at least one encryption key from a group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key. Rowney teach the computer system uses a random encryption key which is a symmetric encryption key (col. 13, lines 4-9) and asymmetric key pair such as a public key/private-key key pair where the message encrypted with one key of the key pair may only be decrypted with the other key of the same key pair (col. 13, lines 8-12).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by using an

encryption key to secure a network connection. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Rowney, in order to provide for a network connection, which prevents an unauthorized entry.

Claim 49 is rejected under 35 U.S.C. 103(a) as being unpatentable over Owens, in view of Blumenau, further in view of Dancs and Stevens.

Claim 49: Further, Owens fails to teach a tracking module for time stamping and storing at least one of the groups comprising the data, a digest of at least a portion of the data, and a digital signature of an access system. Stevens teach a timestamp option with the capability to record both IP addresses and time-stamps (pg. 95-96, section 95-96, section 7.4).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to include time-stamping a group. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to form a digest containing all the pertinent information related to a message.

Dancs teaches the use of a cryptographic signature appended to the contents of the smart card (col. 8, lines 28-39).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to use a

signature for an identifier. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to be able to identify an access system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Todd M Jack whose telephone number is 571-272-3823. The examiner can normally be reached on M-Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Todd Jack
Art Unit 2133

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

February 08, 2005